State of Arizona

Department of Economic Security Information Technology Standards	Title: 1-38-0052 Data Sharing Request/Agreement Policy	
Subject: This is the policy that defines the requirements for sharing DES confidential client, employee, employer information (internal and external)	***Effective Date:*** 04/27/05	***Revision:*** 1

1. Summary of Policy Changes

1.1. Original implementation.

2. Purpose

2.1. This policy establishes policy for the effective and efficient implementation of the DES Data Security Policy to ensure the protection and the controlled sharing of data.

3. Scope

3.1. This procedure encompasses all confidential DES data, all DES personnel and non-DES personnel who have access to DES data in performance of their duties; and all persons, DES and non-DES, who have responsibility for maintaining and preserving DES data. Confidential data consists of, but is not limited to, data that can personally identify clients, employees, providers and employers. Non-confidential data consists of, but is not limited to, statistical and aggregate data that is not personally identifiable.

4. Responsibilities

4.1. The DES Director, Deputy Directors, and Assistant Directors are responsible for implementing and enforcing this policy

4.2. The DES CIO and the Division of Technology Services are responsible for implementing this policy.

5. Definitions and Abbreviations

5.1. Definitions

5.1.1. **Memorandum of Understanding (MOU):** A document that is intended to replace the Data Sharing Agreement for internal entities to share data.

5.1.2. **Need to know:** Having the access to only data that is needed for your job. No more, no less.

5.2. Abbreviations and Acronyms

5.2.1. **GITA - G**overnment **I**nformation **T**echnology **A**gency
5.2.2. **ARS - A**rizona **R**evised **S**tatutes
5.2.3. **DES** – **D**epartment of **E**conomic **S**ecurity
5.2.4. **DTS** – **D**ivision of **T**echnology **S**ervices
5.2.5. Information Technology Standards **ET** – DES **E**xecutive **T**eam
5.2.6. **IT** – **I**nformation **T**echnology
5.2.7. **ITSP - I**nformation **T**echnology **S**trategic **P**lan
5.2.8. **CIO** – **C**hief **I**nformation **O**fficer
5.2.9. **ASLAPR** – AZ **S**tate **L**ibrary, **A**rchives and **P**ublic **R**ecords

6. Policy

6.1. Statement of Policy

Confidential data maintained by DES may be shared only with those individuals or entities, both DES and non-DES, with an established need for access based upon federal and state laws, regulations and directives. Inter-governmental agreements (IGAs) and agent contracts can be used to support the sharing of confidential information. Access to DES confidential data, outside of the program responsible for the data, shall be permitted based on the creation and approval of a Data Sharing Agreement between parties, a DES Memorandum of Understanding or written permission from the Director of the Department of Economic Security, applied to the appropriate situation mentioned below.

The DES Director has been identified as the owner of all DES data. The Director has designated Assistant Directors and Program Administrators in the organization where the data originates as managers or custodians of the data. (See DES Information Security Policy 1-38-0004) These Data Managers are responsible for approving or denying requests for access.

Assistant Directors and Program Administrators will work together to ensure that the sharing of data occurs when needed in accordance with the DES Data Security Policy. Data Managers and the Information Security Administration shall periodically review the data sharing agreements to ensure that they comply with the DES Data Security Policy.

6.2. **Internal Agreement Policy**

It will not be necessary to initiate the Data-Sharing Agreement for data access between internal DES entities once a Memorandum of Understanding is completed for all Divisions. All DES entities will share data based on the “NEED TO KNOW” principle and applicable Federal and State laws, regulations and directives.

The Memorandum of Understanding (MOU) will facilitate the sharing of data internal to all DES Divisions and Programs without having to maintain separate Data Sharing Agreements between Divisions. All Divisions and Programs covered under the MOU will still be required to follow DES IT Policies and Standards regarding account access and authorization approval. A new MOU shall be executed when a personnel change in the Assistant or Deputy Director occurs.

6.3. **HIPAA Requirements** (Health Insurance Portability & Accountability Act)

Confidential data maintained by DES and subject to the requirements of the Health Insurance Portability and Accountability Act (HIPAA) must be documented in the data sharing agreement (J-119) and the request must be reviewed and recommended for approval by the HIPAA Division Privacy Officer. The data sharing agreement will stipulate that all users will read and sign a User Affirmation Statement (J-129) and complete HIPAA level training based on job responsibilities and tasks performed.

6.4. **External Agreement Policy**

One-time requests from non-DES entities asking for statistical or aggregate data shall be submitted to the appropriate program within DES for approval or denial. These requests become the responsibility of the program.

Requests from non-DES entities that require access to DES confidential client, provider, employee or employer information must be approved using the Data Sharing Agreement process. Contracts with non-DES entities shall include, as required, a Business Associate Agreement. These requests can be categorized as follows:

6.4.1. Entities that have contracted with DES and require access to specific information or application(s) controlled by **one** DES entity.

The Data Sharing Agreement process will be initiated and controlled by the appropriate DES entity. The signed document will be forwarded to the Information Security Administration for final DES approval. A non-DES User Identification String will be assigned and security access to the appropriate security analysts will be provided by the ISA. All access by these non-DES users will be totally controlled by the appropriate security analysts.

6.4.2. Entities that have partnered with DES to perform a service and require access to specific information or application(s) controlled by **one** DES organization.

The Data Sharing Agreement process will be initiated and controlled by the appropriate DES entity. The signed document will be forwarded to the Information Security Administration for final DES approval. A non-DES User Identification String will be assigned and security access to the appropriate security analysts will be provided by the ISA. All access by these non-DES users will be totally controlled by the appropriate security analysts.

6.4.3. Federal, State and Local entities that have an Inter-Governmental Agreement (IGA) with DES.

The data sharing agreement process will be initiated by the Information Security Administration. The ISA will work with the non-DES entity representative and when required, the appropriate security analyst(s) will be consulted for advice and information. Each included DES entity will approve or deny access and the ISA will provide final DES approval or denial. Denials will be handled as outlined in the access denial portion (Conflict Resolution) of this document. The ISA will assign a non-DES User Identification String and coordinate all access activity.

6.4.4. Entities that have contracted with DES and require access to information or application(s) controlled by multiple DES organizations.

The Data Sharing Agreement process will be initiated by the Information Security Administration. The ISA will work with the non-Des entity representative and when required, the appropriate security analyst(s) will be consulted for advice and information. Each included DES entity will approve or deny access and the ISA will provide final DES approval or denial. Denials will be handled as outlined in the access denial portion (Conflict Resolution) of this document. The ISA will assign a non-DES User Identification String and coordinate all access activity.

6.4.5. Non-DES entities that request DES information based on the fact that this information can improve their ability to accomplish job responsibilities. An example might be a parent-aid who is contracted by DCYF to help case managers.

The Data Sharing Agreement process will be initiated by the Information Security Administration. The ISA will work with the non-Des entity representative and when required, the appropriate security analyst(s) will be consulted for advice and information. Each included entity will approve or deny access and the ISA will provide final DES approval or denial. Denials will be handled as outlined in the access denial portion (Conflict Resolution) of this document. The ISA will assign a non-DES User Identification String and coordinate all access activity.

6.4.6. All other situations will be handled in the same manner **as 6.4.5**

6.5. Information Technology and Connectivity

6.5.1. Requester documents the automation environment by
providing names, addresses, telephone numbers and e-mail addresses of IT contacts.

6.5.2. DES IT staff reviews the requester's information, works with the requester contact(s) and suggests automation and connectivity options.

6.5.3. DES IT staff documents the accepted process by listing requirements, hardware, software, responsibilities, and if possible, estimate dates and monetary costs.

6.6. **Cost Recovery**

Each DES Division and/or Program incurs internal administrative expense when processing a data sharing agreement. In addition, there is access control expense, training expense, and computer usage expense. The DES Division/Program will decide if cost recovery is mandated by statue. All cost recovery is the responsibility of the DES Division/Program and any cost documents will be attached as an addendum to the data sharing agreement. Data sharing approvals and denials will have no direct relation to cost recovery. If the requester is entitled to the data by statute or regulation and passes the "Need to Know" principle, approval should be granted and the appropriate organization can stipulate that access is provided immediately or after payment of documented expenses.

6.7. **Conflict Resolution**

Disputes, between DES entities and/or outside organizations, should be initiated at the Division/Program Security Analyst level. If it cannot be resolved at this level, the Program Administrators and the Chief Information Security Officer will attempt to resolve the dispute. The next level will be the respective Assistant Director(s) and the Chief Information Security Officer. The DES Director will be the final authority in this process. However, no agreement will be allowed to circumvent the laws, regulations and directives that govern the confidentiality of DES data.

6.8. **Data Sharing Agreement Amendment**

A data sharing agreement must be amended or replaced when the terms of the agreement are changed. A change can be initiated by either party to the agreement. The data security analyst must review the specifics and determine if a new data sharing agreement should be initiated or the access change can be covered in an amendment. The amendment is processed on form J-119 Amendment and is signed by both parties. All amendments will use the data sharing agreement number with the suffix of A1, A2, A3, etc.

6.9. **Data Sharing Agreement Termination**

All data sharing agreements are active for a period of two years unless specified differently in the agreement and agreed to by both parties. Access is provided until the termination date. If access is required for a longer period of time, it is the responsibility of the requesting entity (DES & non-DES) to contact the appropriate security analyst or the Information Security Administration and request that the agreement be renewed. The data security analyst of the appropriate entity will review the data sharing agreement and either provides a data sharing agreement renewal form (see amendment form), a letter of renewal or rejection of the request. The renewal term will be for two years unless specified differently and agreed to by both the parties. The data sharing renewal will use the data sharing agreement number with the suffix of R1, R2, R3, etc.

6.10. **Data Sharing Agreement Expiration**

Terminations can be initiated by the DES Division/Program at any time during the term of the data sharing agreement based on documented violations of the agreement's stipulations. The requesting entity may terminate the agreement at any time by submitting a signed letter to the management of the DES Division/Program.

7. Implications

This policy replaces all previous DES policy on the topic of Data Sharing Requests/Agreements.

8. Implementation Strategy

This policy is effective immediately.

9. References

None

10. Attachments

None

11. Associated GITA IT Standards or Policies

None

12. Review Date

This document will be reviewed twelve (12) months from the original adoption date, and every twelve months thereafter.